VN-0140US

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of
Takayuki SATO
Appln. No. 09/682,122 Group Art Unit:
Filed: July 25, 2001 Examiner: Unknown
For: **MULTI-UNIT BUILDING WITH SECURE ENTRY SYSTEM**

SUBMISSION OF PRIORITY DOCUMENT(S)

Commissioner for Patents
Washington, D.C. 20231

Sir,

Under the provisions of 35 USC 119 and 37 CFR 1.55(a), the applicant hereby claims the right of priority based on the following application(s):

Country	Application No.	Filed
Japan	2001-109776	April 09, 2001

A certified copy of the above-noted application(s) is (are) attached hereto.

Respectfully submitted,

Karan Singh
Registration No. 38698
RYUKA IP LAW FIRM
6th Floor, Toshin Building, 1-24-12,
Shinjuku, Shinjuku-ku, Tokyo, Japan
Telephone: +81-3-5366-7377
Facsimile: +81-3-5366-7288
Date: September 11, 2001

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年　４月　９日

出願番号
Application Number: 特願２００１－１０９７７６

出願人
Applicant(s): アライドテレシス株式会社

２００１年　５月２５日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号　出証特２００１－３０４１８３９

【書類名】　特許願
【整理番号】　IP214010
【提出日】　平成13年 4月 9日
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 17/60
【発明者】
　【住所又は居所】　東京都品川区西五反田７－２２－１７　ＴＯＣビル　アライドテレシス株式会社内
　【氏名】　佐藤　貴之
【特許出願人】
　【識別番号】　396008347
　【氏名又は名称】　アライドテレシス株式会社
【代理人】
　【識別番号】　100104156
　【弁理士】
　【氏名又は名称】　龍華　明裕
　【電話番号】　(03)5366-7377
【手数料の表示】
　【予納台帳番号】　053394
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　集合建築物

【特許請求の範囲】

【請求項１】　部内者のみに進入が許容される閉塞空間が複数設けられた集合建築物であって、

当該集合建築物のコンピュータネットワークシステムを統括的に管理する管理サーバと、

前記管理サーバと、前記閉塞空間において使用されるネットワーク機器とを中継する中継機器と

を備え、

前記管理サーバは、前記複数の閉塞空間のそれぞれに対して異なる前記ＶＬＡＮを割り当てるべく、前記中継機器を設定することを特徴とする集合建築物。

【請求項２】　前記閉塞空間への進入しようとする進入者から、当該進入者の識別情報を取得し、前記識別情報に基づいて、前記進入者が前記部内者であるか否かを認証し、前記部内者のみに前記閉塞空間への進入を許容する利用者認証部をさらに備えることを特徴とする請求項１に記載の集合建築物。

【請求項３】　前記管理サーバは、前記閉塞空間の利用者の前記閉塞空間への進入と、前記利用者による前記ネットワーク機器の前記コンピュータネットワークシステムへの進入とを管理することを特徴とする請求項１に記載の集合建築物。

【請求項４】　前記管理サーバは、前記複数の閉塞空間のそれぞれに対して、前記閉塞空間の識別情報である閉塞空間識別情報を割り当て、

前記閉塞空間は、当該閉塞空間に割り当てられた前記閉塞空間識別情報を有する前記利用者の進入を許容することを特徴とする請求項３に記載の集合建築物。

【請求項５】　前記管理サーバは、前記複数の閉塞空間に割り当てられた前記ＶＬＡＮのそれぞれに対して、前記ＶＬＡＮの識別情報であるＶＬＡＮ識別情報を割り当て、前記ＶＬＡＮに対して割り当てられた前記ＶＬＡＮ識別情報を送信した前記ネットワーク機器の前記コンピュータネットワークシステムへの進入を許容することを特徴とする請求項３に記載の集合建築物。

【請求項６】　前記管理サーバは、前記閉塞空間の利用者の前記閉塞空間への進入と、前記利用者による前記ネットワーク機器の前記コンピュータネットワークシステムへの進入との履歴を記憶することを特徴とする請求項２に記載の集合建築物。

【請求項７】　前記管理サーバは、前記複数の閉塞空間のそれぞれに対して、前記管理サーバとは異なるＶＬＡＮを割り当てることを特徴とする請求項１に記載の集合建築物。

【請求項８】　前記管理サーバは、前記中継機器に対して、前記管理サーバと同一の前記ＶＬＡＮを割り当てることを特徴とする請求項７に記載の集合建築物。

【請求項９】　前記管理サーバは、前記中継機器の接続ポート毎の通信量及び通信時間の少なくとも一方を、前記中継機器から取得し、取得した前記通信量及び前記通信時間の少なくとも一方に基づいて、前記接続ポートの通信を制御することを特徴とする請求項１に記載の集合建築物。

【請求項１０】　前記閉塞空間において使用される前記ネットワーク機器による前記コンピュータネットワークシステムへの進入を管理するエントランスサーバをさらに備えることを特徴とする請求項１に記載の集合建築物。

【請求項１１】　前記エントランスサーバは、前記ネットワーク機器の識別情報である機器識別情報を格納するエントランスデータベースを有し、前記エントランスデータベースに格納された前記機器識別情報を有するネットワーク機器の前記コンピュータネットワークシステムへの進入を許容することを特徴とする請求項１０に記載の集合建築物。

【請求項１２】　前記エントランスデータベースは、前記機器識別情報として前記ネットワーク機器のＭＡＣアドレスを格納し、

前記エントランスサーバは、前記エントランスデータベースに格納された前記ＭＡＣアドレスを有する前記ネットワーク機器の前記コンピュータネットワークシステムへの進入を許容することを特徴とする請求項１１に記載の集合建築物。

【請求項１３】　前記ネットワーク機器の前記ＭＡＣアドレスが、前記エントランスデータベースに格納されていると判断した場合に、当該ネットワーク機

器に対して、ＩＰアドレスを割り当てるＤＨＣＰサーバをさらに備えることを特徴とする請求項１２に記載の集合建築物。

【請求項１４】　前記エントランスサーバは、前記ネットワーク機器の利用者の識別情報である利用者識別情報を格納するエントランスデータベースを有し、前記エントランスデータベースに格納された前記利用者識別情報を送信した前記ネットワーク機器の前記コンピュータネットワークシステムへの進入を許容することを特徴とする請求項１０に記載の集合建築物。

【請求項１５】　前記管理サーバは、前記エントランスサーバに対して、前記複数の閉塞空間のそれぞれに割り当てられたそれぞれの前記ＶＬＡＮと通信することができるＶＬＡＮを割り当てることを特徴とする請求項１０に記載の集合建築物。

【請求項１６】　前記複数の閉塞空間のそれぞれにおいて使用される複数の前記ネットワーク機器に、共通の情報を提供する共用サーバをさらに備えることを特徴とする請求項１に記載の集合建築物。

【請求項１７】　前記管理サーバは、前記共用サーバに対して、前記複数の閉塞空間のそれぞれに割り当てられたそれぞれの前記ＶＬＡＮと通信することができるＶＬＡＮを割り当てることを特徴とする請求項１６に記載の集合建築物。

【請求項１８】　前記複数の閉塞空間のそれぞれにおいて使用される複数の前記ネットワーク機器のそれぞれにＩＰアドレスを割り当てるＤＨＣＰサーバをさらに備えることを特徴とする請求項１に記載の集合建築物。

【請求項１９】　前記管理サーバは、前記ＤＨＣＰサーバに対して、前記複数の閉塞空間のそれぞれに割り当てられたそれぞれの前記ＶＬＡＮと通信することができるＶＬＡＮを割り当てることを特徴とする請求項１８に記載の集合建築物。

【請求項２０】　前記閉塞空間は、前記閉塞空間における異常事態を検出し、前記管理サーバに通知する異常検出手段を有し、

前記異常検出手段は、前記ネットワーク機器が接続される前記中継機器の前記接続ポートの他の接続ポートに接続される

ことを特徴とすることを特徴とする請求項１に記載の集合建築物。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、集合建築物に関する。特に本発明は、管理サーバを備えることにより、セキュリティの高いコンピュータネットワークシステムが形成された集合建築物に関する。

【０００２】

【従来の技術】

集合住宅内にルータやハブ等の集線装置を設置することにより、当該集合住宅にＬＡＮが構築された集合住宅管理システムが開発されている。従来の集合住宅管理システムでは、インターネットを介して接続された管理サーバによって、集合住宅内に設置された集線装置を管理することにより、住戸間のセキュリティ及びＬＡＮの外部に対するセキュリティを管理している。

【０００３】

【発明が解決しようとする課題】

しかしながら、従来の集合住宅管理システムでは、インターネットを介して接続された管理サーバによって、集合住宅に構築されたＬＡＮを管理するため、ＬＡＮの外部に対するセキュリティの維持が困難である。また、インターネットを介して接続された管理サーバは、各住戸において使用されるネットワーク機器を詳細に管理をすることが困難である。

【０００４】

そこで本発明は、上記の課題を解決することのできる集合建築物を提供することを目的とする。この目的は特許請求の範囲における独立項に記載の特徴の組み合わせにより達成される。また従属項は本発明の更なる有利な具体例を規定する。

【０００５】

【課題を解決するための手段】

即ち、本発明の第１の形態によると、部内者のみに進入が許容される閉塞空間が複数設けられた集合建築物は、当該集合建築物のコンピュータネットワークシ

ステムを統括的に管理する管理サーバと、管理サーバと、閉塞空間において使用されるネットワーク機器とを中継する中継機器とを備え、管理サーバは、複数の閉塞空間のそれぞれに対して異なるＶＬＡＮを割り当てるべく、中継機器を設定する。

【０００６】

閉塞空間への進入しようとする進入者から、当該進入者の識別情報を取得し、識別情報に基づいて、進入者が部内者であるか否かを認証し、部内者のみに前記閉塞空間への進入を許容する利用者認証部をさらに備えてもよい。

【０００７】

管理サーバは、閉塞空間の利用者の閉塞空間への進入と、利用者によるネットワーク機器のコンピュータネットワークシステムへの進入とを管理してもよい。管理サーバは、複数の閉塞空間のそれぞれに対して、閉塞空間の識別情報である閉塞空間識別情報を割り当て、閉塞空間は、当該閉塞空間に割り当てられた閉塞空間識別情報を有する利用者の進入を許容してもよい。

【０００８】

閉塞空間識別情報は、閉塞空間の出入口に設けられた錠を開閉する鍵の形状であり、錠は、利用者が有する鍵の形状を認証し、閉塞空間は、錠による鍵の形状の認証が成立した場合、利用者の進入を許容してもよい。

【０００９】

管理サーバは、複数の閉塞空間に割り当てられたＶＬＡＮのそれぞれに対して、ＶＬＡＮの識別情報であるＶＬＡＮ識別情報を割り当て、ＶＬＡＮに対して割り当てられたＶＬＡＮ識別情報を送信したネットワーク機器のコンピュータネットワークシステムへの進入を許容してもよい。管理サーバは、閉塞空間の利用者の閉塞空間への進入と、利用者によるネットワーク機器のコンピュータネットワークシステムへの進入との履歴を記憶してもよい。

【００１０】

管理サーバは、複数の閉塞空間のそれぞれに対して、管理サーバとは異なるＶＬＡＮを割り当ててもよい。管理サーバは、中継機器に対して、管理サーバと同一のＶＬＡＮを割り当ててもよい。

【００１１】

管理サーバは、中継機器の接続ポート毎の通信量及び通信時間の少なくとも一方を、中継機器から取得し、取得した通信量及び通信時間の少なくとも一方に基づいて、接続ポートの通信を制御してもよい。

【００１２】

閉塞空間において使用されるネットワーク機器によるコンピュータネットワークシステムへの進入を管理するエントランスサーバをさらに備えてもよい。エントランスサーバは、ネットワーク機器の識別情報である機器識別情報を格納するエントランスデータベースを有し、エントランスデータベースに格納された機器識別情報を有するネットワーク機器のコンピュータネットワークシステムへの進入を許容してもよい。

【００１３】

エントランスデータベースは、機器識別情報としてネットワーク機器のＭＡＣアドレスを格納し、エントランスサーバは、エントランスデータベースに格納されたＭＡＣアドレスを有するネットワーク機器のコンピュータネットワークシステムへの進入を許容してもよい。ネットワーク機器のＭＡＣアドレスが、エントランスデータベースに格納されていると判断した場合に、当該ネットワーク機器に対して、ＩＰアドレスを割り当てるＤＨＣＰサーバをさらに備えてもよい。

【００１４】

エントランスサーバは、ネットワーク機器の利用者の識別情報である利用者識別情報を格納するエントランスデータベースを有し、エントランスデータベースに格納された利用者識別情報を送信したネットワーク機器のコンピュータネットワークシステムへの進入を許容してもよい。管理サーバは、エントランスサーバに対して、複数の閉塞空間のそれぞれに割り当てられたそれぞれのＶＬＡＮと通信することができるＶＬＡＮを割り当ててもよい。

【００１５】

複数の閉塞空間のそれぞれにおいて使用される複数のネットワーク機器に、共通の情報を提供する共用サーバをさらに備えてもよい。管理サーバは、共用サーバに対して、複数の閉塞空間のそれぞれに割り当てられたそれぞれのＶＬＡＮと

通信することができるＶＬＡＮを割り当ててもよい。

【００１６】

複数の閉塞空間のそれぞれにおいて使用される複数のネットワーク機器のそれぞれにＩＰアドレスを割り当てるＤＨＣＰサーバをさらに備えてもよい。管理サーバは、ＤＨＣＰサーバに対して、複数の閉塞空間のそれぞれに割り当てられたそれぞれのＶＬＡＮと通信することができるＶＬＡＮを割り当ててもよい。

【００１７】

閉塞空間は、閉塞空間における異常事態を検出し、管理サーバに通知する異常検出手段を有し、異常検出手段は、ネットワーク機器が接続される中継機器の接続ポートの他の接続ポートに接続されてもよい。

【００１８】

なお上記の発明の概要は、本発明の必要な特徴の全てを列挙したものではなく、これらの特徴群のサブコンビネーションも又発明となりうる。

【００１９】

【発明の実施の形態】

以下、発明の実施形態を通じて本発明を説明するが、実施形態はクレームにかかる発明を限定するものではなく、また実施形態の中で説明されている特徴の組み合わせの全てが発明の解決手段に必須であるとは限らない。

【００２０】

図１は、本発明の一実施形態に係る集合建築物２００の構成を示す。本実施形態に係る集合建築物２００は、部内者のみに進入が許容される閉塞空間２０が複数設けられており、集合建築物２００のコンピュータネットワークシステムを統括的に管理する管理サーバ１０と、管理サーバ１０と閉塞空間２０において使用されるネットワーク機器２４とを中継する中継機器１２とを備える。

【００２１】

また、集合建築物２００は、集合建築物２００のコンピュータネットワークシステムとインターネットとを接続するルータ１６をさらに備える。ネットワーク機器２４は、ルータ１６を介してインターネットを利用することができる。また、インターネット上に設けられた管理装置が、管理サーバ１０及び管理データベ

ース１４を管理してもよい。

【００２２】

管理サーバ１０は、複数の閉塞空間２０のそれぞれに対して異なるＶＬＡＮを割り当てるべく、中継機器１２を設定する。また、閉塞空間２０は、当該閉塞空間２０に進入する利用者を認証する利用者認証部２２を有する。また、閉塞空間２０は、ハブ等の集線装置２６を有し、閉塞空間２０において集線装置２６に接続された複数のネットワーク機器２４がコンピュータネットワークシステムに接続してもよい。

【００２３】

管理サーバ１０は、複数の閉塞空間２０のそれぞれに対して、閉塞空間２０の識別情報である閉塞空間識別情報を割り当てる。また、管理サーバ１０は、複数の閉塞空間２０のそれぞれに割り当てられたＶＬＡＮのそれぞれに対して、ＶＬＡＮの識別情報であるＶＬＡＮ識別情報を割り当てる。そして、管理サーバ１０は、複数の閉塞空間２０のそれぞれに対応づけて、閉塞空間識別情報及びＶＬＡＮ識別情報を格納する管理データベース１４を有する。

【００２４】

管理サーバ１０は、閉塞空間２０の利用者の閉塞空間２０への進入と、利用者によるネットワーク機器２４のコンピュータネットワークシステムへの進入とを管理する。閉塞空間２０において利用者認証部２２は、管理データベース１４に基づいて利用者が有する閉塞空間識別情報を認証し、当該閉塞空間２０の閉塞空間識別情報を有する利用者のみに当該閉塞空間２０への進入を許容する。

【００２５】

また、管理サーバ１０は、管理データベース１４に基づいて閉塞空間２０のネットワーク機器２４から送信されたＶＬＡＮ情報識別情報を認証し、当該閉塞空間２０に割り当てられたＶＬＡＮのＶＬＡＮ識別情報を送信したネットワーク機器２４にのみコンピュータネットワークシステムへの進入を許容する。

【００２６】

また、管理サーバ１０は、閉塞空間２０の利用者の当該閉塞空間２０への進入と、利用者によるネットワーク機器２４のコンピュータネットワークシステムへ

の進入との履歴を記憶してもよい。管理サーバ１０は、利用者の当該閉塞空間２０への進入と、ネットワーク機器２４のコンピュータネットワークシステムへの進入との履歴を記憶することにより、閉塞空間２０への不正進入及びコンピュータネットワークシステムへの不正進入を検出することができる。

【００２７】

また、閉塞空間２０は、当該閉塞空間２０において発生した火災、ガス漏れ等の異常事態を検出する異常検出手段を有する。異常検出手段は、中継機器１２を介して管理サーバ１０に接続され、検出した異常事態を管理サーバ１０に通知する。そして、管理サーバ１０は、管理者又はセキュリティサービス会社等に通知する。異常事態検出手段は、閉塞空間２０のネットワーク機器２４が接続される中継機器１２の接続ポートと異なる接続ポートに接続されることが好ましい。ネットワーク機器２４と異常検出手段とが異なる接続ポートに接続されることによって、ネットワーク機器２４の誤作動によって異常検出手段が誤作動することを防止することができる。

【００２８】

また、利用者認証部２２は、閉塞空間２０へ進入しようとする進入者から、当該進入者の識別情報を取得し、識別情報に基づいて、進入者が部内者であるか否かを認証し、部内者のみに閉塞空間２０への進入を許容してもよい。また、利用者認証部２２は、閉塞空間２０の出入口に設けられた錠であってもよく、閉塞空間識別情報は、錠を開閉するための鍵の形状であってもよい。錠は、閉塞空間２０の利用者が有する鍵の形状を認証し、錠による鍵の形状の認証が成立した場合、前記利用者の閉塞空間２０への進入を許容してもよい。

【００２９】

また、管理サーバ１０は、例えば管理室などの管理閉塞空間内に配置されてもよい。そして、管理閉塞空間は、当該管理閉塞空間に進入する利用者を認証する利用者認証部を有し、管理サーバ１０は、管理データベース１４に基づいて、利用者による管理閉塞空間への進入を制限してもよい。

【００３０】

本実施形態の集合建築物２００によれば、利用者の閉塞空間２０への進入を制

限し、さらにネットワーク機器２４によるコンピュータネットワークへの進入を制限することにより、コンピュータネットワークへの不正な進入に対して高いセキュリティを実現することができる。

【００３１】

図２は、管理データベース１４に格納される管理情報ファイルのデータフォーマットを示す。管理情報ファイルは、閉塞空間、閉塞空間識別情報、及びＶＬＡＮ識別情報のフィールドを有する。閉塞空間フィールドは、閉塞空間２０を識別する情報を格納する。閉塞空間識別情報フィールドは、閉塞空間２０毎に割り当てられ、閉塞空間２０の利用者を認証するための閉塞空間識別情報を格納する。ＶＬＡＮ識別情報フィールドは、閉塞空間２０のＶＬＡＮ毎に割り当てられ、ＶＬＡＮの利用者を認証するためのＶＬＡＮ識別情報を格納する。管理サーバ１０は、管理データベース１４に基づいて、閉塞空間２０の利用者の閉塞空間２０への進入と、利用者によるネットワーク機器２４のコンピュータネットワークシステムへの進入とを管理する。

【００３２】

図３は、本実施形態に係る集合建築物２００のコンピュータネットワークシステムの構成を示す。本実施形態に係る集合建築物２００のコンピュータネットワークシステムは、閉塞空間２０において使用されるネットワーク機器２４のコンピュータネットワークへの進入を管理するエントランスサーバ３０と、複数の閉塞空間２０において使用される複数のネットワーク機器２４のそれぞれにＩＰアドレスを割り当てるＤＨＣＰ（Ｄｙｎａｍｉｃ　Ｈｏｓｔ　Ｃｏｎｆｉｇｕｒａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）サーバ４０と、複数の閉塞空間２０のそれぞれにおいて使用される複数のネットワーク機器２４に共通の情報を提供する共有サーバ５０とをさらに備える。

【００３３】

管理サーバ１０は、当該管理サーバ１０に対して、管理ＶＬＡＮ１００を割り当てる。また、管理サーバ１０は、中継機器１２に対して、当該管理サーバ１０と同一の管理ＶＬＡＮ１００を割り当てる。したがって、管理サーバ１０は、管理ＶＬＡＮ１００において中継機器１２を制御し、中継機器１２の接続ポートの

ＶＬＡＮ設定を行うことができる。

【００３４】

また、管理サーバ１０は、複数の閉塞空間２０のネットワーク機器のそれぞれに対して、管理ＶＬＡＮ１００とは異なる個別ＶＬＡＮ１１０ａ、１１０ｂ、１１０ｃ、及び１１０ｄを割り当てる。したがって、管理サーバ１０は、閉塞空間２０において使用されるネットワーク機器２４と通信を行うことができない。また、所定の閉塞空間２０において使用されるネットワーク機器２４は、他の閉塞空間２０において使用されるネットワーク機器２４と通信を行うことができない。また、管理サーバ１０は、エントランスサーバ３０、ＤＨＣＰサーバ４０、及び共有サーバ５０に対して、複数の閉塞空間２０のそれぞれに割り当てられた個別ＶＬＡＮ１１０ａ、１１０ｂ、１１０ｃ、及び１１０ｄと通信することができる全体ＶＬＡＮ１２０を割り当てる。

【００３５】

また、管理サーバ１０は、中継機器１２の接続ポート毎の通信量及び通信時間の少なくとも一方を、中継機器１２から取得する。そして、管理サーバ１０は、取得した通信量及び通信時間の少なくとも一方に基づいて、接続ポートの通信を制御する。また、管理サーバ１０は、取得した通信量及び通信時間の少なくとも一方に基づいて、課金情報を生成してもよい。管理サーバ１０は、中継装置１２の接続ポートの通信を制御することによって、当該接続ポートに接続されたネットワーク機器２４によるインターネットへの接続等を制限することができる。

【００３６】

エントランスサーバ３０は、ネットワーク機器２４の識別情報である機器識別情報を格納するエントランスデータベース３２を有する。エントランスデータベース３２は、機器識別情報の一例としてＭＡＣアドレスを格納する。エントランスサーバ３０は、エントランスデータベース３２に格納されたＭＡＣアドレスを有するネットワーク機器２４のコンピュータネットワークシステムへの進入を許容する。ネットワーク機器２４の利用者は、ネットワーク機器２４を用いてエントランスサーバ３０にログインし、ネットワーク機器２４のＭＡＣアドレスをエントランスデータベース３２に登録する。また、エントランスサーバ３０の管理

者が、エントランスサーバ３０を用いてネットワーク機器２４のＭＡＣアドレスをエントランスデータベース３２に登録してもよい。

【００３７】

また、エントランスデータベース３２は、ネットワーク機器２４の利用者の識別情報である利用者識別情報を格納してもよい。そして、エントランスサーバ３０は、エントランスデータベース３２に格納された利用者識別情報に基づいて、ネットワーク機器２４から送信された利用者識別情報を認証してもよい。そして、エントランスサーバ３０は、利用者の認証が成立した場合に、利用者識別情報を送信したネットワーク機器２４のＭＡＣアドレスをエントランスデータベース３２に格納してもよい。そして、エントランスサーバ３０は、利用者識別情報を送信したネットワーク機器２４のコンピュータネットワークシステムへの進入を許容してもよい。

【００３８】

また、ＤＨＣＰサーバ４０は、エントランスデータベース３２に格納されたＭＡＣアドレスを有するネットワーク機器２４に対して、ＩＰアドレスを割り当ててもよい。ＤＨＣＰサーバ４０が、エントランスデータベース３２に登録されたネットワーク機器２４のみにＩＰアドレスを割り当てることによって、登録されたネットワーク機器２４のみがインターネットを使用することができる。

【００３９】

図４は、エントランスデータベース３２に格納されるエントランスファイルのデータフォーマットを示す。エントランスファイルは、閉塞空間、ユーザＩＤ、パスワード、及びＭＡＣアドレスのフィールドを有する。閉塞空間フィールドは、閉塞空間２０を識別する情報を格納する。ユーザＩＤフィールドは、ネットワーク機器の利用者の識別情報である利用者識別情報を格納する。パスワードフィールドは、利用者識別情報で識別される利用者を認証するためのパスワードを格納する。ＭＡＣアドレスフィールドは、それぞれの閉塞空間２０において使用されるネットワーク機器２４のＭＡＣアドレスを格納する。

【００４０】

ユーザＩＤフィールドに格納される利用者識別情報、及びパスワードフィール

ドに格納されるパスワードは、ネットワーク機器の利用者又はネットワーク管理者によって予め登録される。そして、ＭＡＣアドレスフィールドに格納されるＭＡＣアドレスは、ネットワーク機器２４から受信したＭＡＣアドレスが格納される。ネットワーク機器の利用者は、ネットワーク機器を用いてエントランスサーバ３０にログインし、ユーザＩＤ及びパスワードを入力する。そして、エントランスサーバ３０は、入力されたユーザＩＤ及びパスワードを、ユーザＩＤフィールドに格納される利用者識別情報、及びパスワードフィールドに格納されるパスワードによって認証した後、ネットワーク機器２４から受信した当該ネットワーク機器のＭＡＣアドレスを格納する。

【００４１】

また、エントランスデータベース３２は、閉塞空間２０に対応づけてＭＡＣアドレスを格納しており、エントランスサーバ３０は、所定の閉塞空間２０において、当該所定の閉塞空間２０に対応づけて格納されるＭＡＣアドレスを有するネットワーク機器２４のみにコンピュータネットワークシステムへの進入を許容する。

【００４２】

図５は、ＭＡＣアドレス登録処理のフローチャートを示す。まず、エントランスサーバ３０は、中継機器１２に接続されたネットワーク機器２４のＭＡＣアドレスを中継機器１２から受信する（Ｓ１００）。次に、エントランスサーバ３０は、エントランスサーバ３０にログインしたネットワーク機器２４から、当該ネットワーク機器２４において利用者によって入力されたユーザＩＤ及びパスワードを受信する（Ｓ１０２）。次に、エントランスサーバ３０は、エントランスデータベース３２を参照し（Ｓ１０４）、受信したユーザＩＤ及びパスワードを認証する（Ｓ１０６）。Ｓ１０６において、認証が成立しなかった場合、エントランスサーバ３０は、ＭＡＣアドレスの登録処理を終了する。また、Ｓ１０６において、認証が成立した場合、エントランスサーバ３０は、受信したＭＡＣアドレスをエントランスデータベース３２に登録する（Ｓ１０８）。

【００４３】

図６は、ＭＡＣアドレス照合処理のフローチャートを示す。まず、中継機器１

２は、当該中継機器１２に接続されたネットワーク機器２４に電源が投入されたことを検知し、エントランスサーバ３０に通知する（Ｓ２００）。次に、エントランスサーバ３０は、中継機器１２に接続されたネットワーク機器２４のＭＡＣアドレスを中継機器１２から受信する（Ｓ２０２）。次に、エントランスサーバ３０は、エントランスデータベース３２を参照し（Ｓ２０４）、受信したＭＡＣアドレスが格納されているか否かを判断する（Ｓ２０６）。

【００４４】

受信したＭＡＣアドレスがエントランスデータベース３２に格納されている場合、エントランスサーバ３０は、ＤＨＣＰサーバ４０に対して、受信したＭＡＣアドレスを有するネットワーク機器２４へのＩＰアドレスの割り当てを許可する（Ｓ２０８）。そして、ＤＨＣＰサーバ４０は、エントランスサーバ３０の指示に基づいて、ネットワーク機器２４にＩＰアドレスを割り当てる。また、エントランスサーバ３０は、中継機器１２に対して、受信したＭＡＣアドレスを有するネットワーク機器２４が接続された中継機器１２の接続ポートの通信を許可する（Ｓ２１０）。

【００４５】

また、受信したＭＡＣアドレスがエントランスデータベース３２に格納されていない場合、エントランスサーバ３０は、ＤＨＣＰサーバ４０に対して、受信したＭＡＣアドレスを有するネットワーク機器２４へのＩＰアドレスの割り当てを禁止する（Ｓ２１２）。また、エントランスサーバ３０は、中継機器１２に対して、受信したＭＡＣアドレスを有するネットワーク機器２４が接続された中継機器１２の接続ポートの通信を禁止する（Ｓ２１４）。また、エントランスサーバ３０は、受信したＭＡＣアドレスを有するネットワーク機器２４によるコンピュータネットワークシステムへの不正進入であると判断し、受信したＭＡＣアドレスを記憶する（Ｓ２１６）。また、エントランスサーバ３０は、ネットワーク機器２４によるコンピュータネットワークシステムへの不正進入を管理者に通知してもよい。

【００４６】

本実施形態の集合建築物２００によれば、管理サーバ１０、エントランスサー

バ３０、ＤＨＰＣサーバ４０、及び共有サーバ５０を備えることにより、中継機器１２及びネットワーク機器２４の詳細な管理を行うことができる。さらに、インターネットを介さずに中継機器１２及びネットワーク機器２４の管理を行うことにより、セキュリティの高いコンピュータネットワークシステムを構築することができる。さらに、登録されたネットワーク機器２４のＭＡＣアドレスに基づいて、コンピュータネットワークシステムを使用できるネットワーク機器２４を制限することにより、コンピュータネットワークシステムへの不正な進入を防ぐことができる。

【００４７】

以上、本発明を実施の形態を用いて説明したが、本発明の技術的範囲は上記実施形態に記載の範囲には限定されない。上記実施形態に、多様な変更または改良を加えることができる。そのような変更または改良を加えた形態も本発明の技術的範囲に含まれ得ることが、特許請求の範囲の記載から明らかである。

【００４８】

【発明の効果】

上記説明から明らかなように、本発明によれば、管理サーバを備えることにより、セキュリティの高いコンピュータネットワークシステムが形成された集合建築物を提供することができる。

【図面の簡単な説明】

【図１】

本発明の一実施形態に係る集合建築物２００の構成図である。

【図２】

管理データベース１４に格納される管理情報ファイルのデータフォーマットである。

【図３】

本実施形態に係る集合建築物２００のコンピュータネットワークシステムの構成図である。

【図４】

エントランスデータベース３２に格納されるエントランスファイルのデータフ

ォーマットである。

【図５】

ＭＡＣアドレス登録処理のフローチャートである。

【図６】

ＭＡＣアドレス照合処理のフローチャートである。

【符号の説明】

１０　管理サーバ

１２　中継機器

１４　管理データベース

１６　ルータ

２０　閉塞空間

２２　利用者認証部

２４　ネットワーク機器

３０　エントランスサーバ

３２　エントランスデータベース

４０　ＤＨＣＰサーバ

５０　共有サーバ

１００　管理ＶＬＡＮ

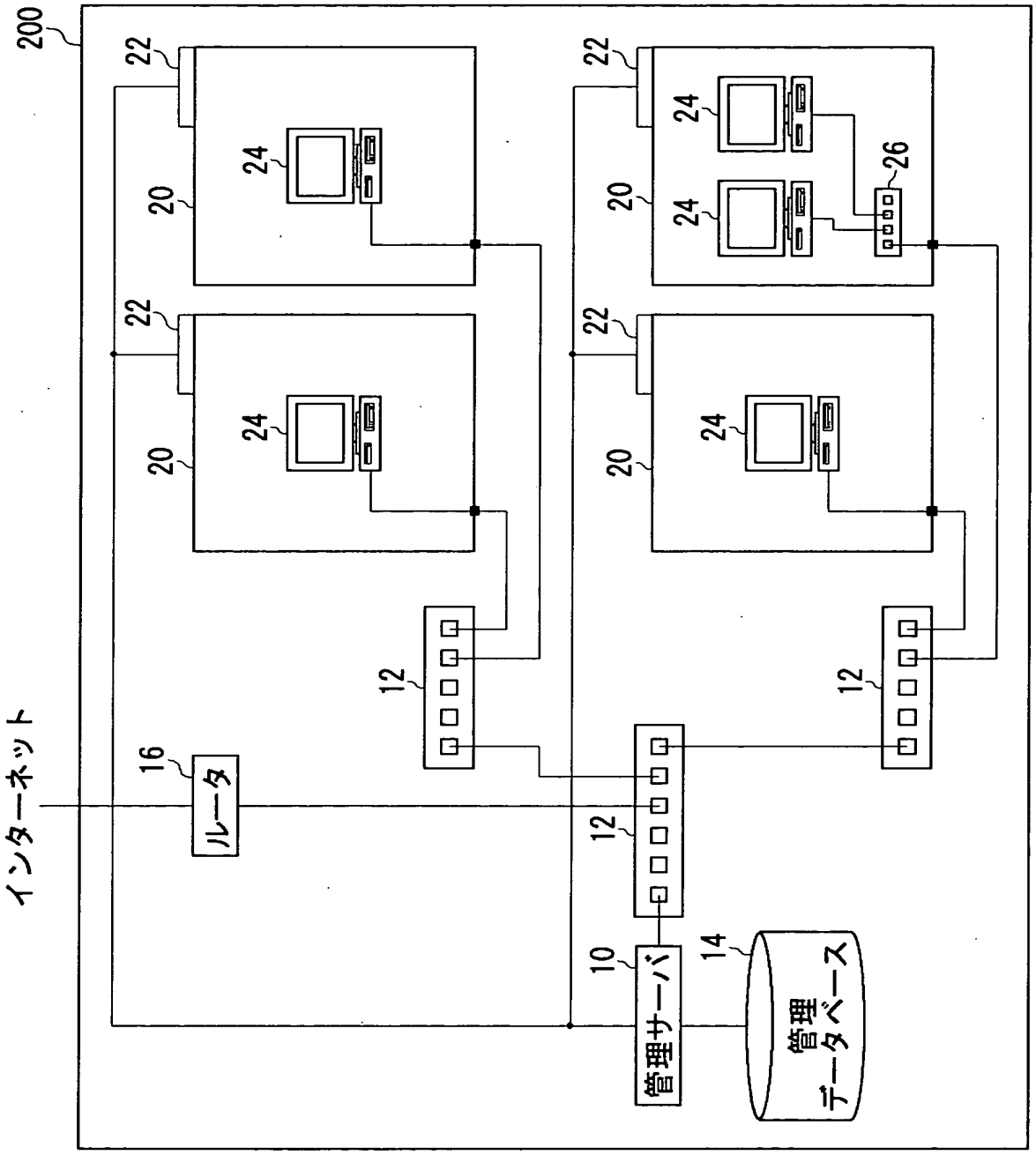
１１０　個別ＶＬＡＮ

１２０　全体ＶＬＡＮ

２００　集合建築物

【書類名】　図面

【図１】



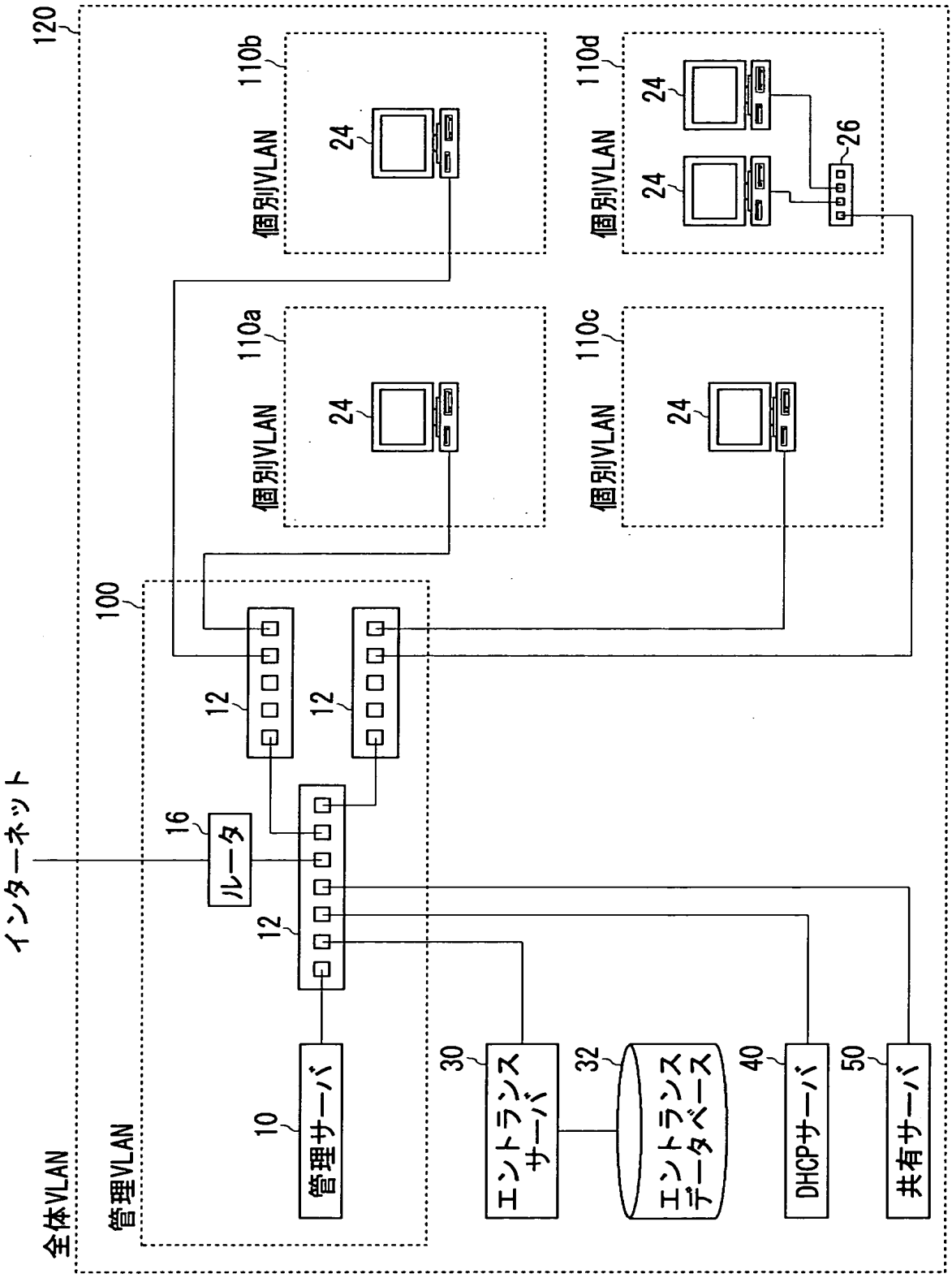
【図２】

14

閉塞空間	閉塞空間識別情報	VLAN識別情報
101	ABCDE	87326
102	FGHIJ	75981
201	LMNOP	67125
202	QRSTU	66719
・ ・ ・	・ ・ ・	・ ・ ・

出証特２００１－３０４１８３９

【図３】

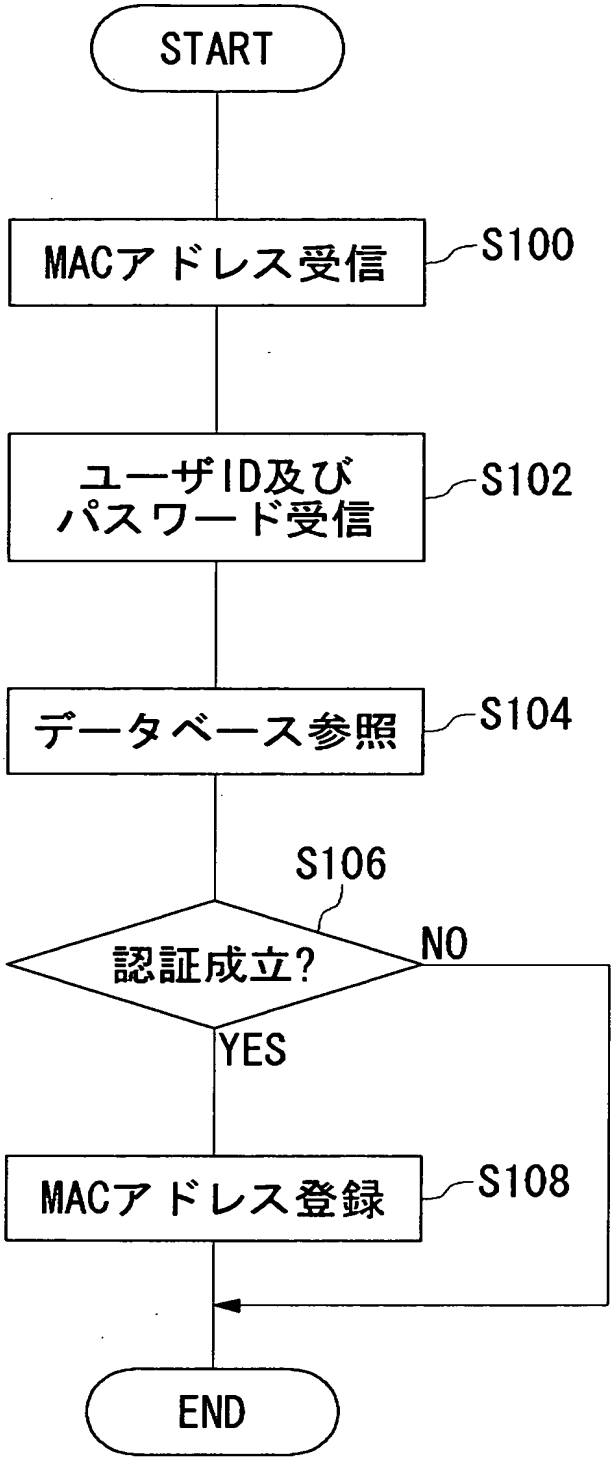

120
110b
個別VLAN
24
110d
個別VLAN
24
24
26
110a
個別VLAN
24
110c
個別VLAN
24
100
12
12
インターネット
16
ルータ
12
全体VLAN
管理VLAN
10
管理サーバ
30
エントランスサーバ
32
エントランスデータベース
40
DHCPサーバ
50
共有サーバ

【図４】

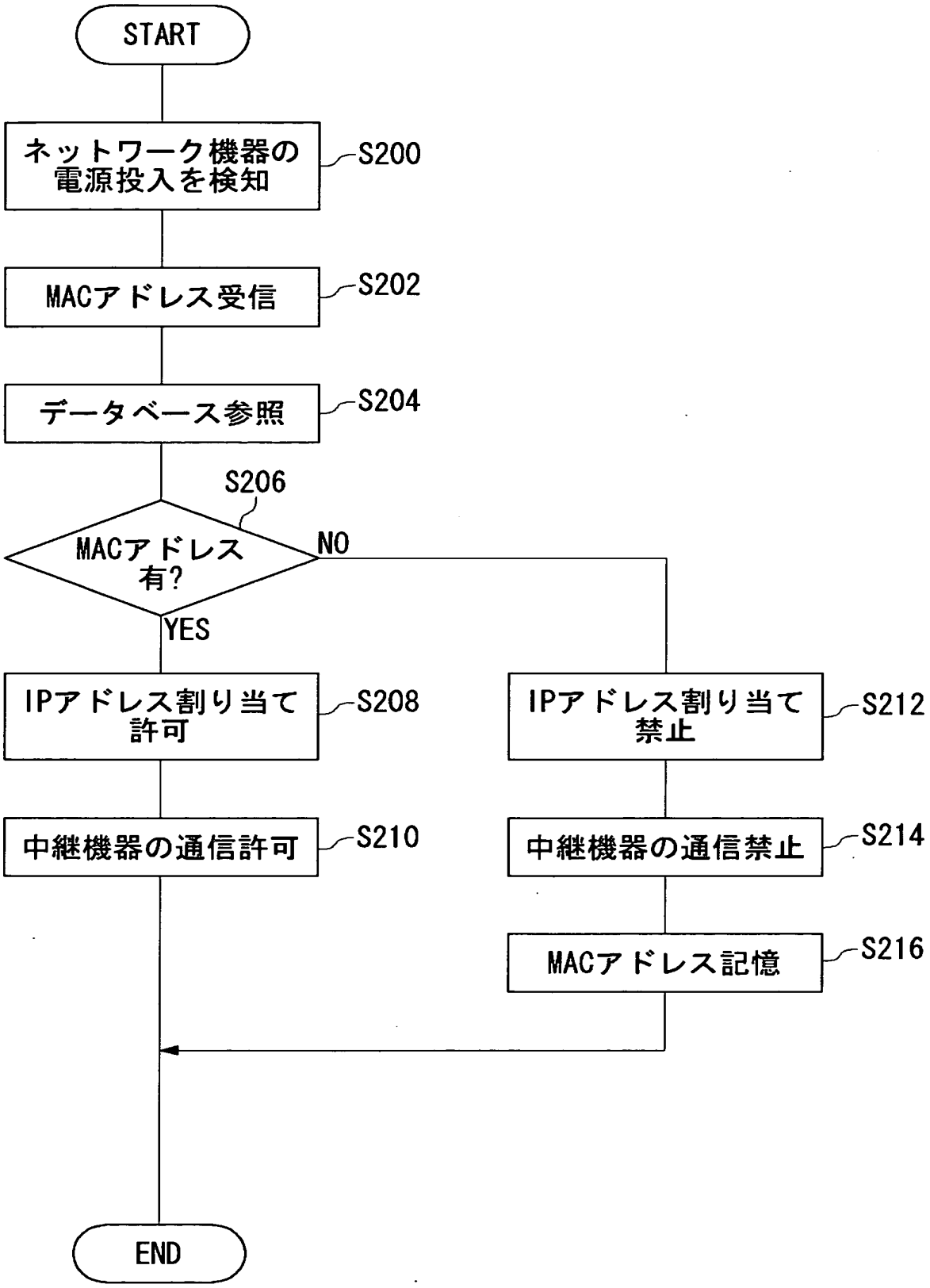
32

閉塞空間	ユーザID	パスワード	MACアドレス
101	aaaaa	*****	50-22-37-AB-66-83
102	bbbbb	*****	33-51-86-CD-76-10
201	ccccc	****	55-01-27-EF-60-11
202	ddddd	*****	61-00-10-GF-51-20
	eeee	*****	53-11-02-HI-12-35
・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・

【図５】


START
MACアドレス受信
S100
ユーザID及び
パスワード受信
S102
データベース参照
S104
S106
認証成立?
NO
YES
MACアドレス登録
S108
END

【図６】


START
ネットワーク機器の電源投入を検知
S200
MACアドレス受信
S202
データベース参照
S204
S206
MACアドレス有?
NO
YES
IPアドレス割り当て許可
S208
IPアドレス割り当て禁止
S212
中継機器の通信許可
S210
中継機器の通信禁止
S214
MACアドレス記憶
S216
END

【書類名】　要約書

【要約】

【課題】　管理サーバを備えることにより、セキュリティの高いコンピュータネットワークシステムが形成された集合建築物を提供する。

【解決手段】　部内者のみに進入が許容される閉塞空間が複数設けられた集合建築物であって、当該集合建築物のコンピュータネットワークシステムを統括的に管理する管理サーバと、管理サーバと、閉塞空間において使用されるネットワーク機器とを中継する中継機器とを備え、管理サーバは、複数の閉塞空間のそれぞれに対して異なるＶＬＡＮを割り当てるべく、中継機器を設定する。

【選択図】　図２

出　願　人　履　歴　情　報

識別番号　　〔３９６００８３４７〕

１．変更年月日　　２０００年１０月２４日
［変更理由］　住所変更
住　所　東京都品川区西五反田７－２２－１７　ＴＯＣビル
氏　名　アライドテレシス株式会社